UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS

@Shu Qian/Unsplash

I-Soon leaks : coup d'œil sur un cyberarsenal chinois

Par Alexis Rapin

Première en son genre, une importante fuite de documents met à nu les activités d'une firme technologique employée par l'appareil sécuritaire chinois. Mine d'or pour les services de contre-espionnage, celle-ci révèle des cibles inattendues, mais aussi une boîte à outils bien fournie.

La NSA américaine a connu les révélations d'Edward Snowden en 2013. Le renseignement russe a subi la divulgation des *Vulkan files* en 2023. La Chine, de son côté, aura désormais les *I-Soon leaks*. Apparue le mois dernier sur la plateforme de partage de fichiers GitHub, cette importante fuite de documents livre en effet un aperçu inédit des activités d'I-Soon, une entreprise technologique contractante de l'appareil sécuritaire chinois. Au gré de plusieurs centaines de fichiers, on y découvre notamment des fiches techniques d'outils de cybersurveillance, des listes de cibles du renseignement chinois, ou encore des potins de bureau échangés par les employés de cette mystérieuse officine.

Selon différentes firmes de cybersécurité occidentales, I-Soon travaillerait principalement pour le ministère de la Sécurité publique (MPS) de la République populaire, l'organe chargé de traquer les dissidents et de surveiller les minorités jugées « problématiques » (tels les Ouïghours) par Pékin. C'est depuis la métropole sichuanaise de Chengdu, pôle majeur du secteur numérique chinois, qu'opérerait l'entreprise. Dans ce torrent de révélations explosives, un seul mystère demeure : l'origine de la fuite. Là où certains analystes envisagent la possibilité qu'elle puisse provenir d'une firme compétitrice ou d'un service de renseignement étranger, d'autres penchent plutôt pour l'hypothèse d'un employé mécontent ayant disséminé ces secrets en guise de vengeance. Sans présumer de sa source, que peut-on néanmoins apprendre en passant en revue cette mine d'information privilégiée ?

Parts de marché

Les *I-Soon leaks* révèlent en premier lieu des listes d'entités visées par le MPS, dont le contenu s'avère à bien des égards surprenant. D'une part, on découvre que l'essentiel de celles-ci sont basées à l'étranger, alors que le MPS a théoriquement pour mandat historique de veiller à la sécurité intérieure de la République populaire. Or, de la Thaïlande à la Guinée en passant par le Royaume-Uni, les activités d'I-Soon ne se limitent pas aux frontières chinoises. Certaines sources estiment néanmoins que l'entreprise pourrait travailler aussi pour le ministère de la Sécurité d'État (MSS), quant à lui tourné vers l'étranger. Un fait intéressant à cet égard est qu'une part importante des cibles évoquées dans les fuites se situent dans les pays de l'Association des nations de l'Asie du Sud-Est, bien davantage que dans les grandes puissances occidentales réputées préoccuper Pékin en priorité.

Il est néanmoins probable que les efforts d'I-Soon soient loin de refléter l'ensemble des activités de renseignement de la Chine : d'autres contractants similaires ont probablement pour mission de se concentrer sur des pays comme les États-Unis, la France ou le Canada. De fait, certains documents contenus dans la fuite révèlent un marché des contractants gouvernementaux extrêmement compétitifs, dans lequel tous les coups sont permis pour remporter des appels d'offres de l'appareil sécuritaire. Le terrain couvert par I-Soon pourrait donc n'être qu'un « périmètre de chasse » parmi bien d'autres dans le grand écosystème du cyberespionnage chinois.

Suivre l'argent

Les cibles d'I-Soon s'avèrent surprenantes pour d'autres raisons également : on y observe en effet une forte attention consacrée à des pays partenaires, voire alliés de Pékin. C'est le cas notamment du Pakistan (principal associé de la Chine dans sa rivalité avec l'Inde voisine), dont différentes entités gouvernementales apparaissent dans les listes d'I-Soon. Mais c'est bien davantage à l'encontre de ses partenaires africains que la République populaire déploie d'importants efforts de surveillance, de l'Afrique du Sud à l'Éthiopie, en passant

par Djibouti et la République démocratique du Congo. Ce ciblage peut néanmoins s'expliquer; il s'agit là des pays africains dans lesquels l'empire du Milieu a le plus investi dans les dernières années. Le cyberespionnage de Pékin semble donc en partie consacré à surveiller étroitement ses débiteurs.

Un autre élément tend à accréditer cette thèse, à savoir la liste des pays européens visés par I-Soon. De fait, les mentions faites de la Macédoine du Nord, de la Roumanie ou encore de la Bosnie peuvent de prime abord surprendre compte tenu du faible poids géopolitique de ces États. On remarque néanmoins que ce sont là quelques-uns des pays européens à avoir pris part à la Belt & Road Initiative, le grand projet de nouvelles routes de la soie promu par l'empire du Milieu. Là aussi, l'attention des services de renseignement semble donc s'aligner fortement sur les lignes de crédit ouvertes par Pékin. Une preuve de plus, s'il en fallait une, que pour la Chine l'économie est un enjeu de sécurité nationale à part entière.

Gadgets en prime

Au-delà de ces cibles, les *I-Soon leaks* laissent aussi entrevoir une petite partie de la boîte à outils numérique du renseignement chinois, qui n'a, semble-t-il, pas grand-chose à envier à ses homologues américains ou russes. On y découvre entre autres plusieurs logiciels espions pensés pour compromettre des appareils utilisant Windows, iOS et Android ainsi qu'un outil visant à pirater des comptes Outlook. Un autre logiciel permet d'identifier le courriel ou le numéro de téléphone se cachant derrière un compte X (anciennement Twitter), ou même d'en scruter les messages personnels.

Fait intéressant, les catalogues d'I-Soon contiennent également divers gadgets permettant

©Kandukuru Nagarjun/Wikipedia commons

de compromettre des appareils « en présentiel ». Y figure par exemple un boîtier ressemblant à un chargeur portatif, mais qui, lorsqu'activé dans le périmètre d'un wifi, permet de craquer celui-ci pour épier les autres appareils y étant connectés. Un autre dispositif paraît quant à lui dédié à sécuriser des communications émises depuis l'étranger. La firme de Chengdu semble donc aussi contribuer à équiper les agents de l'appareil sécuritaire chinois déployés sur le terrain.

Un appareil contraint malgré tout

En définitive, les *I-Soon leaks* nous livrent surtout un aperçu du fonctionnement de l'écosystème du renseignement chinois qui, à l'instar de ceux de bien d'autres États, se révèle de plus en plus sous-traité, voire privatisé. On y voit I-Soon se disputer des contrats gouvernementaux avec d'autres entreprises, pour des marges de profit d'ailleurs très limitées. Des PowerPoint léchés servent de matériel promotionnel pour les armes numériques de la firme. Divers messages montrent des mandataires presser les délais de livraison. Des employés se plaignent de leur paie et disent envisager de rejoindre d'autres industries.

Les *I-Soon leaks* dépeignent ainsi un monde du renseignement chinois s'apparentant à un marché comme un autre, régi par les lois de la concurrence et de la rentabilité. Resterait évidemment à savoir combien d'I-Soon compte au total l'appareil sécuritaire chinois, et si tous travaillent dans les mêmes conditions. Un constat important s'en dégage néanmoins : généralement considéré par ses adversaires comme disposant de moyens colossaux, l'appareil d'espionnage chinois reste visiblement lui aussi contraint dans la gestion de ses ressources.

Alexis Rapin est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : https://dandurand.uqam.ca.

@Kristoffer Trolle/Flickr